

**AFFIDAVIT IN SUPPORT OF AN APPLICATION
FOR A SEARCH WARRANT**

I, Terrance L. Taylor, being first duly sworn, hereby depose and state as follows:

INTRODUCTION

1. I am a Special Agent with the United States Department of Homeland Security, Homeland Security Investigations (“HSI”). I have been so employed since March 2012. I am currently assigned to the Office of the Resident Agent in Charge HSI Charleston, West Virginia. I have experience in conducting investigations involving computers and the procedures that are necessary to retrieve, collect, and preserve electronic evidence. Through my training and experience, including on-the-job discussions with other law enforcement agents and cooperating suspects, I am familiar with the operational techniques and organizational structure of child pornography distribution networks and child pornography possessors and their use of computers and other media devices.

2. Prior to my employment with HSI, I was a Police Officer for two years in Huntington, West Virginia, a Special Agent with the United States Department of State-Bureau of Diplomatic Security for six years, a Special Agent with the Naval Criminal Investigative Service for two years, and a Special Agent with the United States Department of State-Office of Inspector General for two years. I am a graduate of three federal law enforcement academies at the Federal Law Enforcement Training Center (“FLETC”) and a graduate of the West Virginia State Police Academy. I graduated from the Criminal Investigator Training Program in 2002, and the Immigration and Customs Enforcement Special Agent Training Program in 2012. As part of these programs, I received extensive training in the areas of law within the jurisdiction of HSI. I

have specifically received training in the areas of child pornography and the sexual exploitation and abuse of children. This training includes specialized instruction on how to conduct criminal investigations related to violations of child protection laws pursuant to Title 18, United States Code, Sections 2251, 2252, 2252A, and 2256.

3. As a Special Agent, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I have gained experience through training at the FLETC, Immigration and Customs Enforcement, as well as everyday work relating to investigations involving the receipt, possession, access with intent to view, production, importation, advertising, and distribution of child pornography that occur in the District of Southern West Virginia. I have received training in the areas of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media, including computer media. I have obtained search warrants for child pornography offenses, and I have been the case agent or assisted others in numerous investigations involving the sexual exploitation of children. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2252A(a)(2) (receipt or distribution of child pornography), and 2252A(a)(5)(B) (possession of child pornography), and I am authorized by law to request a search warrant.

4. I make this affidavit in support of an application for a search warrant for information associated with a certain Snapchat username that is stored at premises owned, maintained, controlled, or operated by Snap Inc. ("Snap"), a social networking company headquartered in Santa Monica, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for

a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Snap to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B, related to a Snapchat account for the username alienated5555 (the “Subject Account”). Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

5. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

6. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 2252A (transport, receipt, distribution, possession, and access with intent to view child pornography) (the “Subject Offenses”), have been committed by Jerry Dewayne Carroll (“CARROLL”). There is also probable cause to search the information described in Attachment A for evidence, contraband, and/or fruits of these crimes further described in Attachment B.

BACKGROUND ON SNAPCHAT¹

7. Snap, Inc. (“Snap”) the owner of Snapchat, is a United States company and a provider of an electronic communications service as defined by 18 U.S.C. §§ 3127(1) and 2510. Specifically, Snapchat is a free-access social networking service, accessible through its website and its mobile application, that allows subscribers to acquire and use Snapchat accounts like the

¹ The information in this section is based on information published by Snap on its website, including, but not limited to, the following document and webpages: “Snap Inc. Law Enforcement Guide,” available at <https://storage.googleapis.com/snap-inc/privacy/lawenforcement.pdf>; and “Snapchat Support,” available at <https://support.snapchat.com/>.

Subject Account listed in Attachment A, through which users can share messages, multimedia, and other information with other Snapchat users.

8. Snap collects basic contact and personal identifying information from users during the Snapchat registration process. Snap also collects whether the account phone number has been verified.

9. Snap also collects and retains information about how each user accesses and uses Snapchat. This includes information about the Internet Protocol (“IP”) addresses used to create and use an account, unique identifiers and other information about devices and web browsers used to access an account, and session times and durations. Snap also collects account change history, which Snap describes as a log of changes in registration email or phone number, birthdate, and display name.

10. Each Snapchat account is identified by a username.

11. Snapchat offers four primary ways for users to communicate with each other.

a. **Snaps.** A user takes a photo or video using their camera phone in real-time. The user then selects a time limit of 1-10 seconds for the receiver to view the photo or video. A user can elect to have the photo/video saved in their phone’s photo gallery or just sent via Snapchat, without being saved. The photo/video can then be sent to a friend in Snapchat. The snap is deleted after the selected amount of time. If a recipient attempts to take a screenshot of the snap to save on his/her phone, the application will notify the sender of this behavior. Snapchat states that it deletes each snap from its servers once all recipients have

viewed it. If a snap has not been viewed by all recipients, Snapchat states that it retains the snap for thirty days.

b. **Memories.** Memories is Snapchat's cloud-storage service. Users can save their sent or unsent Snaps, posted Stories, and photos and videos from their phone's photo gallery in Memories. A user can also edit and send Snaps and create Stories from these Memories. Snaps, Stories, and other photos and videos saved in Memories are backed up by Snapchat and may remain in Memories until deleted by the user.

c. **Stories.** A user can also add the photo/video Snap to their "Story." Depending on the user's privacy settings, the photos and videos added to a Story can be viewed by either all users of Snapchat or just the user's friends for up to 24 hours. Stories can also be saved in Memories.

d. **Chat.** A user can also type messages to friends within the Snapchat app using the Chat feature. A user sends a Chat message to a friend, and once it is viewed by both parties – and both parties swipe away from the Chat screen – the message will be cleared. Within the Snapchat app itself, a user can opt to save part of the Chat by tapping on the message (text or photo) that he or she wants to keep. The user can clear the message by tapping it again.

12. Snapchat also obtains a variety of non-content information from its users.

13. **Usage Information.** Snapchat may collect information about how users interact with its services, including which search queries they submit, and how they communicate with other users, including maintaining a log of all snaps to and from an account for the last 31 days,

for 24 hours of posted Stories, and for any unopened Chats or those saved by a sender or recipient, and how a user interacts with these messages (such as when a user opens a message).

14. **Device Information.** Snapchat collects information about the devices of its users, including information about the user's hardware and software, such as the hardware model, operating system version, device memory, advertising identifiers, unique application identifiers, apps installed, unique device identifiers, browser type, language, battery level, and time zone; information from device sensors, such as accelerometers, gyroscopes, compasses, microphones, and whether the user has headphones connected; and information about the user's wireless and mobile network connections, such as mobile phone number, service provider, and signal strength. Snapchat can also provide the version of the application that is being used, the "last active" date the application was used, and whether two-factor-authentication is enabled.

15. **Device Phonebook.** Snapchat may collect information about the phonebook of the user's device.

16. **Cameras and Photos.** Snapchat may collect images and other information from the user's device's camera and photos.

17. **Location Information.** Snapchat may collect information about the user's location, including precise location using methods that include GPS, wireless networks, cell towers, Wi-Fi access points, and other device sensors, such as gyroscopes, accelerometers, and compasses.

18. **Snap Map.** Snapchat allows a user to share location information with his/her friends and also obtain location information about the user's friends. Based on such information,

Snapchat places the friends' locations on a map viewable to the user. Snapchat can provide whether Snap Map was enabled.

19. **Information Collected by Cookies and Other Technologies.** Snapchat may collect information through cookies and other technologies about the user's activity, browser, and device.

20. **Log Information.** Snapchat collects log information when a user uses Snapchat's website, including device information, access times, pages viewed, IP address, and pages visited.

21. In my training and experience, evidence of who was using the above listed usernames and from where, and evidence related to the Subject Offenses, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

22. The stored communications and files connected to a Snapchat account may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation. In fact, evidence is included in this affidavit detailing the use of Snapchat by CARROLL to commit the Subject Offenses.

23. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Snap can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs,

documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

24. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

25. Therefore, Snap's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Snapchat. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

PROBABLE CAUSE

26. On or about January 16, 2023, Snapchat submitted CyberTipline Report #152857798 to the National Center for Missing and Exploited Children ("NCMEC"). The incident type was identified as apparent child pornography, and the incident time was listed as: January 15, 2023, at 18:05:59 UTC.

27. Snapchat uploaded two files in connection with the report, each containing

apparent child pornography. Snapchat reported that the files at issue were uploaded by Snapchat username "alienated5555," email address ALIENATED2323@GMAIL.COM, date of birth 07-xx-19xx, and IP address 47.213.82.125.

28. On or about January 16, 2023, your Affiant reviewed the two files associated to the CyberTip and found those to contain the following: (1) an image depicting a white, nude, prepubescent female, approximately 3-5 years old, performing fellatio on a white, adult male; and (2) an image depicting a white, nude, prepubescent female lying on her back; the image focused on her naked vagina and semen was observed on her leg and vagina.

29. Further investigation revealed that the IP address provided in the Cybertip, 47.213.82.125, resolved to Suddenlink Communications. The account listed the subscriber as Phillip Mace with an account address of 121 Hastings Drive, Belle, WV 25015, and a phone number of 304-949-3276.

30. Law enforcement was able to link both Phillip Mace and Toni Mace to the residence using driver's licenses databases. Law enforcement was able to determine that Phillip Mace and Toni Mace were married.

31. On March 7, 2023, a federal search warrant was obtained to search the 121 Hastings Drive residence belonging to Phillip and Toni Mace. The search warrant was executed on March 16, 2023.

32. During the search warrant execution Toni Mace agreed to speak with your Affiant. Your Affiant advised Toni Mace of the federal search warrant regarding the search and seizure of her electronic devices to include cellphones, computers, and external storage devices. Toni Mace stated she understood and advised that her husband, Phillip Mace, was currently in the hospital for

medical issues. No other individuals live at the residence.

33. Toni and Phillip Mace's son, Phillip Mace II, died due to drug dependence issues in October 2022. Toni Mace advised that their son lived down the street at 125 Hastings Drive, Belle, West Virginia ("125 Hastings Drive residence"). Phillip and Toni Mace own the residence and allowed their son and his fiancé, Cynthia Ellis ("Ellis"), to live there. After her son's death, Ellis continued to reside at the 125 Hastings Drive residence.

34. Toni Mace stated she and her husband use Suddenlink/Optimum as their internet service provider. They have a Wi-Fi router that is password protected. She further advised that the Wi-fi could be accessed from both the 121 Hastings Drive residence, as well as the 125 Hastings Drive residence where her son had lived prior to his death. Toni Mace further advised that she was aware that her deceased son accessed the internet using her Suddenlink/Optimum Wi-Fi and password at the 125 Hastings Drive residence. When Toni Mace changed the locks on the 125 Hastings Drive residence recently, she found her Wi-Fi router name and password taped to the window within the 125 Hastings Drive residence.

35. Toni Mace advised that since her son's death in October 2022, a man she knew as J.D. Carroll lived with Ellis at the 125 Hastings Drive residence.

36. Through further investigation, law enforcement was able to link the man Toni Mace knew as J.D. Carroll to CARROLL. CARROLL was issued a West Virginia driver's license bearing the name Jerry Dewayne CARROLL (#F097645), with a date of birth as July xx, 19xx. This date of birth matches the date of birth Snapchat provided for user alienated5555, as indicated in the Cypertip.

37. Law enforcement analysts were further able to link the email address

ALIENATED2323@GMAIL.COM from the Cybertip to CARROLL.

38. On or about March 20, 2023, a preservation request was sent to Snap regarding the Subject Account as well as an administrative subpoena for subscriber information for the Subject Account. Snap issued reference number 236924180 regarding the preservation request. Furthermore, Snap identified the Subject Account as previously being reported to the NCMEC for child exploitation activities.

39. On April 7, 2023, a federal search warrant was obtained to search the person of CARROLL. The search warrant was executed on April 10, 2023. During the search warrant execution, one electronic device was seized from CARROLL's person, specifically a One Plus cellphone.

40. On April 10, 2023, CARROLL was arrested in Kanawha County, West Virginia on a West Virginia state warrant issued from Putnam County, West Virginia, and he has remained detained since that time.

41. The One Plus cellphone was subsequently forensically reviewed. The phone contained 1,400 images of child pornography. Furthermore, the cellphone revealed evidence of the use of Mega. Law enforcement was further able to determine that the Mega account utilized by CARROLL had the username ALIENATED2323@GMAIL.COM. Further, law enforcement found evidence on the One Plus cellphone that this email address had been accessed on the cellphone.

42. On or about May 18, 2023, law enforcement sent a request to Mega for data associated with the Mega account ALIENATED2323@GMAIL.COM to be preserved for 90 days.

43. Mega further provided law enforcement with subscriber and other non-content information regarding the Mega account for ALIENATED2323@GMAIL.COM. This information indicated that the account had been accessed from IP address 47.213.82.125, which is the same IP address identified in the Snapchat Cybertip.

44. On June 6, 2023, a federal search warrant was obtained to search the Mega account ALIENATED2323@GMAIL.COM associated to Jerry Dewayne CARROLL. The search warrant was executed on June 9, 2023. The forensic review of the aforementioned Mega account contained 82 child pornography videos.

45. Subsequent investigation identified the minor child victim associated to the Snapchat CyberTip. The photograph, as described in Paragraph 28, depicted a 3-5 year old female performing fellatio on an unknown adult male. The minor victim was identified by her mother. The minor victim's mother also stated that CARROLL was her cousin and had access to the minor victim in the summer of 2020.

CONCLUSION

46. Based on the foregoing, there is probable cause to believe that evidence related to the Subject Offenses may be located in the information described in Attachment A.

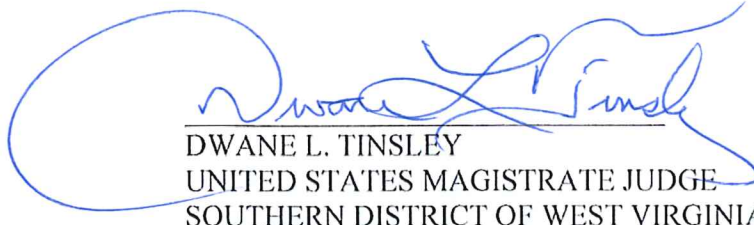
47. Based on the foregoing, I request that the Court issue the proposed search warrant.

48. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Snap. Because the warrant will be served on Snap, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.



Terrance L. Taylor
Special Agent
Department of Homeland Security
Homeland Security Investigations

Sworn to by the Affiant telephonically in accordance with the procedures of Rule 4.1 this
15th day of February, 2024.



DWANE L. TINSLEY
UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF WEST VIRGINIA